

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,
v.
MORTEZA AMIRI,
Defendant.

Case Nos. 23-cr-00264-JSW-2
23-cr-00269-JSW-1

**ORDER DENYING DEFENDANT
AMIRI'S MOTIONS TO SUPPRESS**

~~***PROVISIONALLY UNDER SEAL***~~

Now before the Court are two sister motions to suppress brought by Defendant Morteza Amiri. Amiri moves to suppress all fruits of the searches of his Apple iCloud data pursuant to search warrants issued on February 10, 2022 (3:22-mj-70169 LB) (the "February iCloud Warrant") and March 15, 2022 (3:22-mj-70314-JSC) (the "March iCloud Warrant" and, together, the "iCloud Warrants"), as well as all fruits of the search of his cell phone data pursuant to a warrant issued on March 22, 2022 (3:22-mj-70356) (the "iPhone Warrant").

The Court issues this Order provisionally under seal. The Court ORDERS the parties to file a joint statement regarding whether the Order should remain under seal, including any proposed redactions, within 14 days of this Order.

The Court has considered the parties' papers, relevant legal authority, the record in this case, and oral argument of the parties. For the following reasons, the Court DENIES Amiri's motions.

BACKGROUND

A. February iCloud Warrant: Search Warrant in Case No. 3:22-mj-70169 LB (February 10, 2022).

In 2021, the Federal Bureau of Investigation ("FBI") inquired into officers in the Pittsburgh and Antioch Police Departments, beginning with former Antioch Police Officer

Timothy Manly Williams (“Manly”). FBI Special Agent Thuy Zoback, who has investigated cases involving gangs and drug trafficking since 2009, searched Manly’s Apple iCloud and Instagram accounts pursuant to warrants which are not challenged here. (Dkt. No. 192¹, Government’s Opposition to Amiri’s Motions to Quash and Suppress (“Opp.”), Ex. 1, ¶ 16.) Zoback’s searches revealed conversations between Manly and other police officers—including Amiri—regarding use, exchange, and sale of steroids. Zoback also received, from the Pittsburgh Police Department, two anonymous letters received by the department claiming that Officer Patrick Berhan and “several other officers” were buying and selling steroids “from a doctor in Florida.” (Dkt. No. 174-4, “Affidavit in Support of February iCloud Warrant,” ¶ 41 [US-000600].) Based on these discoveries, Zoback sought to expand the investigation to other officers to uncover potential illicit trafficking of controlled substances.

On February 10, 2022, Zoback applied for a search warrant to find “evidence of a crime” and “contraband, fruits of crime, or other items illegally possessed” within the Apple accounts associated with telephone numbers for Officers Daniel Harris, Armando Montalvo, Patrick Berhan, Calvin Prieto, and Defendant Amiri. (Affidavit in Support of February 2022 Apple iCloud Warrant [US-000579-80].) Zoback believed that the officers violated 21 U.S.C. sections 841(a)(1) (possession with intent to distribute controlled substances) and 846 (conspiracy to distribute controlled substances), and 18 U.S.C. sections 1343, 1346 (honest services wire fraud) and 1349 (conspiracy to commit honest services wire fraud). (*Id.*, ¶ 2 [US-000581].)

The Magistrate Judge agreed with Agent Zoback and signed off on the warrant. (Dkt. No. 189-2, “February iCloud Warrant” [US-000669].)

B. March iCloud Warrant: Search Warrant in Case No. 3:22-mj-70314 JSW (March 15, 2022).

On March 15, 2022, Zoback obtained a warrant to expand the search into the police officers’ iCloud accounts to include evidence of violations of 18 U.S.C. sections 1512(c) (obstruction of justice) and 1519 (destruction of records) (together with the original suspected offenses, “Target Offenses”). (Dkt. No. 174-5, “Affidavit in Support of March iCloud Warrant”

¹ Except where otherwise noted, all docket citations refer to the docket in Case No. 23-cr-264.

[US-000535].) Based on the messages obtained from the first iCloud Warrant, Agent Zoback believed that the subject officers had erased messages or switched to using encrypted messaging software in order to evade detection.

C. iPhone Warrant: Search Warrant in Case No. 3:22-mj-70356 LB (March 22, 2022).

On March 22, 2022, Agent Zoback applied for a more extensive search warrant using information she obtained while executing the iCloud Warrants. (Dkt. No. 174-7, Affidavit in Support of iPhone Warrant” [US-000441].) Zoback added Officers Rombough, [REDACTED] and Montalvo to the list of subject persons, and added violations of 18 U.S.C. sections 1343 (wire fraud) and 1344 (bank fraud) to the list of Target Offenses. (*Id.*)

The Magistrate Judge issued a warrant to search Amiri’s person, mobile phone, iPhone, Apple Watch, and home. (Dkt. No. 174-6, “iPhone Warrant,” Attachment A [US-000385-89].) The warrant permitted the Government to seize “evidence, fruits or instrumentalities” of the Target Offenses. (*Id.*, Attachment B [US-000390].)

The iPhone Warrant specified that law enforcement personnel could require Amiri to unlock his iPhone and other personal electronic devices with his biometric signature or facial recognition, but it did not authorize the personnel to obtain Amiri’s passcode. (*Id.* [US-000392].)

D. Amiri Volunteers His iPhone Passcode.

On March 23, 2022, agents from the Federal Bureau of Investigation (“FBI”) interviewed Amiri at his place of employment, the Antioch Police Department. (Dkt. No. 174-8, Amiri Interview Transcript (“Amiri Tr.”), at 1.) Before reading Amiri his rights pursuant to *Miranda v. Arizona*, 384 U.S. 436 (1966), Special Agent Krystal Templin solicited Amiri’s iPhone passcode. (*Id.* at 3:1-19, 3:25-5:1.) Agent Templin informed Amiri that the FBI had a warrant for Amiri’s phone and that the warrant included “biometrics.” (*Id.* at 3:25.)

Agent Templin then asked Amiri if he would “mind” giving another agent identified as “Joyce” his passcode. (*Id.* at 4:15.) Amiri interrupted Agent Templin and offered his code. (*Id.* at 4:16-17.)

E. Zoback Obtains Additional Warrants.

On April 21, 2022, Zoback applied for and obtained an additional warrant to search

Amiri's iCloud and iPhone data for evidence of violations of 18 U.S.C. sections 241 (conspiracy against rights), 243 (deprivation of rights under color of law), and 1343 (wire fraud). (Dkt. No. 174-9, "Affidavit in Support of First April 2022 Warrant" [US-000875].) Zoback affirmed that "[w]hile agents searched" the data previously obtained pursuant to the iCloud Warrants and the iPhone Warrant for evidence of the alleged steroid scheme, they "observed numerous additional conversations about the potentially excessive use of force by [the warrant] subjects and other officers. Agents also observed numerous additional conversations about wire fraud schemes" relating to falsely obtaining college credits. (*Id.* ¶ 3 [US-000877].)

Agent Zoback affirmed that, in searching the iCloud data, she had found extensive text messages between Amiri and Individual-1² in which Amiri discussed paying Individual-1 to complete college classes on his behalf. (*Id.* ¶¶ 25-38 [US-000887-91].) She also found messages between Amiri, Rombough, and Wenger suggesting that the officers purposely used excessive force in the course of their duties. (*Id.* ¶¶ 12-23 [US-000881-87].)

On April 29, 2022, Zoback applied for yet another warrant to expand the date range of content to be searched and further specifying the electronic devices owned by each subject officer. (Dkt. No. 174-10, "Affidavit in Support of Second April 2022 Warrant" [US-000847].)

F. The Government Charges Amiri with Crimes Unrelated to the Purchase or Sale of Controlled Substances.

Amiri was indicted along with five co-defendants on August 16, 2023 for wire fraud (18 U.S.C. § 1343) and conspiracy to commit wire fraud (18 U.S.C. § 1349) for the alleged college degree scheme. Amiri was indicted on August 16, 2023 along with Rombough and Wenger for violations of 18 U.S.C. sections 241 (conspiracy against rights), 242 (deprivation of rights under color of law), and 1519 (destruction, alteration, and falsification of records).

Although other officers were indicted with charges relating to the alleged steroid scheme, Amiri was not.

² Individual-1's identity is known to the Court and was not redacted in Agent Zoback's affidavit in support of her application for a search warrant. (Affidavit in Support of First April 2022 Warrant, ¶ 25 [US-000887].)

ANALYSIS

Amiri contends that law enforcement lacked probable cause to support the iCloud Warrants and the iPhone Warrant. He further contends that the warrants were overbroad and lacked particularity, and that law enforcement conducted an unconstitutional “exploratory rummaging” that exceeded the warrants’ scope. Finally, Amiri argues that Officer Templin violated his rights by soliciting his iPhone passcode before reciting his *Miranda* rights.

The Government disagrees and contends that law enforcement was scrupulous in obtaining search warrants. It also contends that Amiri volunteered his passcode while not in a custodial interrogation and, even if Agent Templin unlawfully solicited the passcode, that the fruits of his statement constitute physical evidence that may be used.

G. Legal Standards on a Motion to Quash a Search Warrant and Suppress Evidence.

A defendant challenging a warrant as constitutionally infirm must show (1) the warrant was invalid under the Fourth Amendment, or (2) an otherwise valid warrant was “executed in a manner that rendered the searches unreasonable.” *United States v. Artis*, 919 F.3d 1123, 1128 (9th Cir. 2019).

A search warrant satisfies the Fourth Amendment if it is (1) issued by a “neutral, disinterested” magistrate judge; (2) supported by an application that demonstrates probable cause that “the evidence sought will aid in a particular apprehension or conviction for a particular offense”; and (3) describes with particularity the place to be searched and the things to be seized. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal marks omitted).

H. The February iCloud Warrant Was Valid.

Amiri claims that the iCloud Warrants were not supported by probable cause, were vague and overbroad, and that they were executed in an unreasonable manner. The Court disagrees.

The February iCloud Warrant authorized production from Apple of (a) information identifying Amiri’s Apple account associated with his phone number; (b) information identifying the devices associated with Amiri’s Apple account; (c) all emails associated with the account; (d) all instant messages associated with the account; (e) all files and records stored on iCloud; (f) all activity, connection, and transactional logs for the account; (g) location data; (h) all records

1 pertaining to the types of service used; and (i) communications between Apple and others
 2 regarding the account. (February iCloud Warrant, Attachment B [US-000673-74].)

3 From these records, the warrant permitted the FBI to seize:

4 All information described above in Section II that constitutes evidence or
 5 instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with
 6 intent to distribute controlled substances), 846 (conspiracy to distribute
 7 controlled substances), 18 U.S.C. §§ 1343, 1346 (honest services wire
 8 fraud), and/or 1349 (conspiracy to commit honest services wire fraud)
 involving Timothy MANLY WILLIAMS, Daniel HARRIS, Armando
 MONTALVO, Patrick BERHAN, Morteza AMIRI, and/or Calvin PRIETO
 since **October 1, 2019**, specifically, for each account or identifier listed on
Attachment A, information pertaining to the following matters:

- 9 (a) Records and communications indicating the possession, use, purchase, sale,
 10 distribution, transfer, and/or concealment of controlled substances;
- 11 (b) Records and communications indicating any improper influence on official
 12 acts or services, including the receipt, sending, and/or contemplation of any
 benefits, bribes, and/or kickbacks in exchange for any official acts or
 services;
- 13 (c) The identity of the person(s) who created or used the Apple account and/or
 14 Apple ID, including records that help reveal the whereabouts of such
 person(s);
- 15 (d) Evidence indicating how and when the account was accessed or used, to
 16 determine the chronological and geographic context of account access, use
 and events relating to the crime under investigation and the account
 subscriber;
- 17 (e) Any records pertaining to the means and source of payment for services
 18 (including any credit card or bank account number or digital money transfer
 account information);
- 19 (f) Evidence indicating the subscriber's state of mind as it relates to the crime
 20 under investigation; and
- 21 (g) Evidence that may identify any co-conspirators or aiders and abettors,
 22 including records that help reveal their whereabouts.

23 (*Id.* [US-000674-75].)

24 **1. Probable Cause Supported the February iCloud Warrant.**

25 Probable cause supports a search warrant if there is a “fair probability that contraband or
 26 evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238
 27 (1983). “This standard does not require the affidavit to establish that the evidence is in fact in the
 28 place to be searched, or even that it is more likely than not to be there. Rather, the issuing judge

1 need only conclude that it would be reasonable to seek the evidence in the place indicated in the
2 affidavit.” *United States v. Elmore*, 917 F.3d 1068, 1074 (9th Cir. 2019) (internal citations and
3 quotations omitted). “All data necessary to show probable cause” “must be contained within the
4 four corners of a written affidavit given under oath.” *United States v. Gourde*, 440 F.3d 1065,
5 1067 (9th Cir. 2006) (en banc) (quotation and citation omitted).

6 “A magistrate judge’s finding of probable cause is entitled to great deference,” and, upon
7 review, courts “will not find a search warrant invalid if the magistrate judge had a ‘substantial
8 basis’ for concluding that the supporting affidavit established probable cause.” *United States v.*
9 *Crews*, 502 F.3d 1130, 1135 (9th Cir. 2007) (quoting *United States v. Clark*, 31 F.3d 831, 834 (9th
10 Cir.1994)). “[C]ourts should not invalidate warrants by interpreting affidavits in a hypertechnical,
11 rather than a commonsense, manner.” *Gates*, 462 U.S. at 236 (quoting *United States v. Ventresca*,
12 380 U.S. 102, 109 (1965)) (internal marks omitted).

13 Here, Agent Zoback’s application created a substantial basis on which the Magistrate
14 Judge could find probable cause that evidence of illicit drug trafficking would be found in Amiri’s
15 iCloud account.

16 **a. Text Messages Between Manly and Amiri.**

17 Agent Zoback identified one conversation between Manly and Defendant Amiri that he
18 believed referred to Amiri injecting steroids in July 2020:

19 AMIRI: Bro I could barely walk. I’m limping hella hard. From that
20 second shot (slapping forehead emoji)

21 MANLY: Is it a hard spot on the leg?

22 AMIRI: yes, right where I injected

23 AMIRI: feels like I got kneed right there

24 MANLY: I didn’t know you had to inject twice hahaha I would have
told you

25 AMIRI: think I should use your massager on my leg?

26 MANLY: Not really lol... your going to feel that pain for at least a
27 week it sucks remember going through it. took a while for
my body to adjust to it

28 AMIRI: guess I’ll ride it out (crying laughing emoji)

(February 2022 Apple iCloud Warrant, ¶ 44 [US-000600-01].)

Agent Zoback had been investigating Manly for buying and selling steroids, and she had uncovered evidence of Manly distributing steroids illegally to other police officers. Given that context, Amiri's choice to seek advice from Manly regarding pain management after injecting steroids could support a reasonable inference that (1) Amiri obtained the drugs from Manly, and (2) Amiri used his Apple products to communicate with Manly about the drugs. This alone creates a substantial basis to believe that evidence of alleged criminal conduct could be found in Amiri's iCloud account.

b. Instagram Messages Between Manly and Montalvo.

Agent Zoback identified a conversation between Manly and Officer Montalvo in which they referred to Amiri obtaining steroids from a doctor in Florida:

MANLY: Lmao- bro I need a new connect, I had a boy that I worked with but he's out on injury and possible going to medical out and fell off the face of the earth lol

MONTALVO: I can ask around, what are you looking for?

MANLY: Honestly I don't know shit about anything only two I've been running are Test and Deca.... I'm actually comfortable with that I guess unless there's some better shit

MONTALVO: Which test tho?

Cyp? Enth? Prop?

I'm assuming cyp but just want to confirm

MANLY: Have you actually figured this shit out and what's good and what actually works?

I was running this last October it was cool but I had to inject myself damn near everyday which got annoying... I'm just little to cut body weight and gain muscle

MONTALVO: So just trying to cut or also get big?

Also are you doing that Florida thing

MANLY: What's the Florida thing lol

MONTALVO: Lol I heard a bunch of guys with APD we're doing this thing with a Florida doctor to have it prescribed

MANLY: Oooooooooo shit yeah Morteza is doing that right now – I

haven't jumped into

(*Id.* ¶ 45 [US-000601-02].) Agent Zoback interpreted the above conversation between Manly and Montalvo to mean that Manly needed a new supplier in order to obtain steroids. (*Id.*)

Amiri argues that the conversation is, if anything, exculpatory, because obtaining prescription medications is presumably legal. However, Agent Zoback contended, and the Magistrate Judge agreed, that evidence of obtaining a prescription from a doctor on the other side of the country tends to support an inference that the prescription is fraudulent.

c. The Anonymous Letters.

Amiri asserts that the two anonymous letters received by the department claiming that Officer Patrick Berhan and “several other officers” were buying and selling steroids “from a doctor in Florida” were insufficient to create probable cause to search Amiri’s iCloud account. (Affidavit in Support of February iCloud Warrant, ¶ 46 [US-000602].)

Anonymous statements alone do not create probable cause. *Gates*, 462 U.S. at 227 (observing that “something more” may be needed to supplement an anonymous tip). Other corroborating information must be found within the affidavit to bolster the reliability or basis of the anonymous note. *See Artis*, 919 F.3d at 1132 (disregarding statement by unnamed cooperating witness where affidavit provided no information regarding the witness’s reliability nor any corroborating information).

Here, Agent Zoback disclosed that the letters were anonymous and named only Berhan and “several other officers.” (Affidavit in Support of February iCloud Warrant, ¶ 41 [US-000600].) However, the content of the anonymous letters was corroborated by the other evidence uncovered by Zoback. The letters stated that Berhan and other Antioch officers obtained steroids “from a doctor in Florida.” Manly, when reaching out to Montalvo to find a new supplier, acknowledged that “Morteza” was “doing that Florida thing” to have steroids prescribed. (*Id.* ¶ 45 [US-000601-02].) These pieces of information, when read together, support an inference that Amiri was one of the officers buying and selling steroids via a doctor in Florida.

d. Text Messages Between Manly and Prieto.

Amiri further argues that there is no evidence in Agent Zoback’s affidavit to connect Amiri

1 to any allegations of illegal kickbacks or bribes. This assertion is undermined by the text of the
2 affidavit.

3 In the section regarding Prieto, Agent Zoback relayed a conversation between Prieto and
4 Manly in which the two discussed Amiri providing bottles of tequila for a third officer in
5 exchange for the third officer failing to show up to traffic court. (*Id.* ¶¶ 49-55 [US-000603-06].)
6 Manly agreed to make bottles of alcohol “magically appear” if the officer would not skip court so
7 that the driver would not get “a point on his record.” (*Id.*) However, Manly was on vacation out
8 of the country, so he asked Amiri to pass along the bottles:

9 MANLY: I’m up in Cabo...if you working I’ll tell Amiri to bring them

10 PRIETO: Oh fasho fam, enjoy your time

11 MANLY: You want him to bring them to work? Lol

12 I already gave him a heads up

13 PRIETO: Naw we’ll pass by his house

14 We in class all week

15 MANLY: Yeah hit him I already told him you would probably pass
16 through and grab them

17 PRIETO: All good. I’ll hit him up now

18 (*Id.* ¶ 54 [US-000606].)

19 This conversation suggests that Amiri cooperated with Manly and Prieto to facilitate a
20 bribe to an officer to dissuade the officer from performing her duties. An officer executing the
21 warrant could reasonably expect to find further communications, such as between Prieto and
22 Amiri, or Amiri and Manly, in Amiri’s iCloud data that bolster evidence of the scheme.

23 **e. The Cumulation of Allegations Supports Probable Cause.**

24 Mindful of the Supreme Court’s directive that reviewing courts should consider search
25 warrants with “common sense” rather than “hypertechnicality,” *see Gates*, 462 U.S. at 236, the
26 Court finds that the Magistrate Judge had a substantial basis to find probable cause to search
27 Amiri’s iCloud account for evidence of criminal conduct, or the fruits thereof, relating to illegally
28 buying or selling steroids or to improper exchanges for official acts.

The Magistrate Judge was aware of extensive evidence that Manly and the other officers were illegally purchasing, exchanging, and selling steroids. By reading Manly's conversations with and about Amiri in that context, the Magistrate Judge did not impermissibly assume "guilt by association" as Amiri contends. The other officers interacted directly with or referenced by name Amiri when describing obtaining steroids or participating in a kickback scheme.

2. The February iCloud Warrant Was Sufficiently Specific.

Amiri argues that the iCloud Warrants were overly broad and not particularized because, by their terms, the warrants allowed the FBI to access all of Amiri's iCloud data without reference to objective criteria or search parameters. Amiri asserts that, in the absence of particularized categories of data to be searched and search parameters, Agent Zoback conducted an "exploratory rummaging" to find evidence of any possible offenses. (Dkt. No. 176, Mot., 11:14-17.)

The Government counters that Amiri conflates the scope of the authorized search with the scope of the authorized seizure, and that both were reasonable.

"Search warrants must be specific. 'Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.' " *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (quoting *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)). "The level of specificity required 'varies depending on the circumstances of the case and the type of items involved.' " *Id.* (quoting *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986)). "Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Spilotro*, 800 F.2d at 963.

a. The Scope of the Information to Be Obtained from Apple and Reviewed by the FBI Was Permissible.

Digital data presents unique challenges for search warrant breadth. Probable cause must support seizure of all evidence of the particular type described in the warrant. *Spilotro*, 800 F.2d at 963. However, the Ninth Circuit has recognized that "[o]ver-seizing is an accepted reality in electronic searching because there is no way to be sure exactly what an electronic file contains

without somehow examining its contents.” *United States v. Flores*, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (“*CDT*”)) (internal marks omitted). Thus, a two-step seizure in which law enforcement first scoops up large quantities of data and then segregates responsive data is lawful. *CDT*, 621 F.3d at 1177. The warrant need not provide a narrow search protocol if the Government cannot identify the name and location of files to be seized with greater particularity. See *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013) (approving broad review of digital devices where “government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner”).

The February iCloud Warrant included an appropriate two-step data seizure and segregation procedure. In the first step, law enforcement personnel were authorized to “review the information received and identify and copy only the information that [the] search warrant authorizes to be further copied.” (February iCloud Warrant, Attachment B [US-000672].) The remaining information was to be segregated and not reviewed without further court order. (*Id.*)

Additionally, there was a temporal limit in the warrant: the FBI had access to less than three years of iCloud data. This makes the warrant narrower than that approved by the Ninth Circuit in *Flores*, where the court upheld a warrant seizing Facebook data in a two-step process with no time limitations. *Flores*, 802 F.3d at 1045-46. Agent Zoback could not comb through the entirety of Amiri’s iCloud account, because Apple was only required to turn over data from October 2019 through the date of the February iCloud Warrant. (February iCloud Warrant, Attachment B [US-000673].)

b. The February iCloud Warrant Stated the Scope with Particularity.

A search warrant is sufficiently particular if it “sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not,” provided the government was not “able to describe the items more particularly in light of the information available to it at the time the warrant was issued.” *Spilotro*, 800 F.2d at 963. Even if the warrant seeks generic categories of evidence, “[r]eference to a specific illegal act can, in appropriate cases, provide substantive guidance for the officer’s exercise of discretion in executing the warrant.”

1 *Spilotro*, 800 F.2d at 964. The particularity requirement prohibits “the seizure of one thing under
2 a warrant describing another.” *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982) (quoting
3 *Marron v. United States*, 275 U.S. 192, 196 (1927)).

4 Amiri contends that the iCloud Warrants were insufficiently particular because they
5 authorized seizure of categories of evidence akin to those rejected by the Ninth Circuit in other
6 cases. The Government responds that the warrants in each of those cases are distinguishable.

7 In *United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994), the Ninth Circuit held that a
8 search warrant was facially overbroad because it included a “catchall phrase authorizing seizure of
9 ‘fruits and instrumentalities of [a] violation of’” a particular statute, without describing what
10 evidence would qualify as a fruit or instrumentality of the crime. *Id.* at 836 (bracket in original).
11 The court noted that the phrase was not limited or explained by a description in an attached
12 affidavit.

13 Similarly, the Ninth Circuit invalidated a warrant in *United States v. Crozier*, 777 F.2d
14 1376, 1381 (9th Cir. 1985) that authorized seizure of “[m]aterial evidence of violation 21 USC
15 841, 846 (Manufacture and Possession with intent to distribute Amphetamine and Conspiracy).”
16 Although the affidavit specified “Amphetamine, precursor chemicals. . . , laboratory apparatus,
17 notes, formulas, as well as any indicia of ownership and control of the premises,” the affidavit was
18 not attached to the warrant. *Id.* In the absence of any more detail, the warrant “authorize[d] a
19 general search for evidence of an amphetamine business.” *Id.* This was too broad. *Id.*

20 In *Center Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 750 (9th Cir. 1989),
21 the overbroad search warrant authorized seizure of virtually any evidence of “violations of federal
22 criminal law.” *Id.* at 749. The warrant did not limit the scope of the seizures to specific evidence
23 relating to the falsification of Salvador Dali artwork, the suspected crime. *Id.* at 750. Further, the
24 affidavit in support of the warrant was not attached to the warrant, expressly incorporated therein,
25 or given to the defendant as part of the search. *Id.*

26 In *United States v. Cardwell*, the Ninth Circuit held that a warrant was impermissibly
27 vague where it permitted seizure of “books and records” without a “preambulatory statement
28 limiting the search to evidence of particular criminal episodes.” 680 F.2d at 77. The invalid

1 warrant further instructed law enforcement officers to seize “books and records. . . which are the
2 fruits and instrumentalities[] of violations of 26 U.S.C. s 7201.” *Id.* at 76. The court held that,
3 where “items that are illegal, fraudulent, or evidence of illegality are sought, the warrant must
4 contain some guidelines to aid the determination of what may or may not be seized.” *Id.* at 78.
5 The absence of such guidelines was particularly impermissible in *Cardwell* because the IRS had
6 conducted an investigation prior to obtaining a warrant, and it possessed information that it could
7 have, but failed, to use to limit the scope of the warrant. *Id.* In the absence of a preambulatory
8 statement, more precise definitions, and in light of the information already available to the
9 government, the warrant was invalid. *Id.*

10 The warrant in *United States v. Stubbs*, 873 F.2d 210, 212 (9th Cir. 1989) was even more
11 vague. It made no reference to any criminal activity, at all, and instead authorized the seizure of
12 “broad classes of documents without specific description of the items to be seized.” *Id.* The Court
13 stressed that the government “knew both what the seizable documents looked like and where to
14 find them,” but that it did not include the information in the warrant. *Id.* at 211.

15 The warrant in this case differs from those in *Clark*, *Crozier*, *Cardwell*, and *Stubbs*. Here,
16 the February iCloud Warrant did not include a general catchall phrase allowing seizure of
17 evidence of fruits or instrumentalities of violations of a particular statute. Instead, the “evidence
18 or instrumentalities” language in the preambulatory paragraph is limited by the buckets in
19 subparagraphs (a) through (g). (February iCloud Warrant, Attachment B [US-0006174-75].)
20 Thus, the precaution in *Clark*, *Crozier*, *Cardwell*, and *Stubbs* against an expansive catchall phrase
21 is irrelevant.

22 Certain of the categories of evidence authorized for seizure by the February iCloud
23 Warrant may appear overbroad in isolation but are sufficiently particular when considered in
24 context. Unlike the search warrants in the cases cited by Amiri, any facial overbreadth is cured by
25 the preambulatory statement before the list of items to be seized. *See Cardwell*, 680 F.2d at 77
26 (noting preambulatory statement may have cured otherwise overly general categories). Although
27 attachment of Agent Zoback’s affidavit would have added helpful context, there was enough
28 limiting information on the face of the warrant itself to provide guidelines for executing law

1 enforcement agents.

2 The Ninth Circuit in *Cardwell* instructs that courts reviewing the validity of search
3 warrants must “consider the totality of the circumstances” when determining whether a warrant is
4 impermissibly broad—including, importantly, how much information was available to the
5 government at the time it sought the warrant. 680 F.2d at 78. Unlike in *Cardwell*, *Stubbs*, and
6 *Center Art Galleries*, in which the government had more detailed evidence of the materials it
7 sought to obtain, here Agent Zoback had little information to narrow the scope of the search. *See*
8 *id.* at 78 (noting government had knowledge of particular documents to be seized and their
9 location); *Stubbs*, 873 F.2d at 211 (same); *Center Art Galleries*, 875 F.2d at 750 (finding general
10 search impermissible when probable cause supported search relating only to faux Salvador Dali
11 material). Agent Zoback knew that lawful searches of Manly’s phone had revealed records and
12 communications relating to the listed categories, and that further evidence was likely to be found
13 on Amiri’s phone. In her affidavit, Agent Zoback attested that she believed evidence of the drug
14 trafficking scheme would be found in “text messages, email messages, pictures, attachments to
15 emails, attachments to texts, pictures of evidence, pictures of co-conspirators, co-conspirators
16 listed in saved contacts, and calendar events.” (Affidavit in Support of February iCloud Warrant,
17 ¶ 70 [US-000612].) The suspected co-conspirators are named as subjects of the warrant request
18 based on conversations each of the suspects had with Manly. (*Id.* ¶ 11 [US-000583].) This
19 information could have reasonably been found anywhere in Amiri’s iCloud data. *Cf. Schesso*, 730
20 F.3d at 1046 (approving breadth of warrant for electronic data where “[t]he government was faced
21 with the challenge of searching for digital data that was not limited to a specific, known file or set
22 of files.”).

23
24 **c. Probable Cause Supported the Breadth of Each of the Categories of
Records to Be Seized.**

25 As discussed above, the Magistrate Judge had probable cause to issue the February iCloud
26 Warrant. Probable cause likewise supported the scope of authorized seizure.

27 Subparagraphs (a) (records and communications indicating the possession, use, purchase,
28 sale, distribution, transfer, and/or concealment of controlled substances) and (f) (evidence

1 indicating state of mind) are well-supported by the information in Agent Zoback’s affidavit.
2 (February iCloud Warrant, Attachment B [US-000675].) Text messages between Manly and
3 Amiri suggested that Amiri was using steroids; messages between Manly and Prieto suggested that
4 Amiri was fraudulently obtaining steroids from Florida; and two anonymous letters stated that
5 Berhan and other Antioch Police Officers were obtaining and reselling steroids from Florida.
6 (Affidavit in Support of February iCloud Warrant, ¶¶ 45-46 [US-000601-02].) None of these
7 communications illuminates the specific steroids Amiri may have used or sold. Given the limited
8 information available to Agent Zoback, it was reasonable to search for evidence of possession,
9 use, purchase, sale, distribution, transfer, and concealment of controlled substances generally. *See*
10 *United States v. Adjani*, 452 F.3d 1140, 1147-48 (9th Cir. 2006) (“Warrants which describe
11 generic categories of items are not necessarily invalid if a more precise description of the items
12 subject to seizure is not possible.”)

13 Subparagraph (b) (records and communications reflecting illegal kickbacks) is likewise
14 supported by Agent Zoback’s affidavit. Agent Zoback knew from a text conversation between
15 Manly and Prieto that Amiri may have been privy to or participated in effecting a bribe to an
16 officer in exchange for not testifying. (Affidavit in Support of February iCloud Warrant, ¶ 54
17 [US-000606].) The Magistrate Judge thus had a reasonable basis to believe that evidence of
18 kickback schemes could be found in Amiri’s iCloud data.

19 Subparagraphs (c) and (d) (evidence indicating who owned and used the iCloud account,
20 and the timeline of use) are likewise supported by Agent Zoback’s affidavit. In the digital context,
21 evidence of accountholders, time- and geo-stamps, and user IDs is the functional equivalent to
22 indicia of ownership or possession of a tangible object or premises. Search warrants may
23 authorize seizure of non-criminal evidence which demonstrates the connection between the
24 suspect and the premises. *United States v. McLaughlin*, 851 F.2d 283, 286 (9th Cir. 1988).

25 Subparagraph (e) (financial records) is supported by the affidavit’s evidence that Amiri
26 was buying, selling, using, or distributing illicit substances and participation in illegal kickback
27 schemes. Officers could reasonably expect to find evidence of the suspected transactions reflected
28 in Amiri’s financial records, including credit card and digital account transfer information.

Subparagraph (g) (evidence indicating co-conspirators) is supported by the affidavit's identification of suspected co-conspirators and expansive list of potential items which may yield evidence of conspiracy. (Affidavit in Support of February iCloud Warrant, Attachment B [US-000619].) The suspected co-conspirators are named as subjects of the warrant request based on conversations each of the suspects had with Manly. (*Id.* ¶ 11 [US-000583].) This information adequately supports the breadth of category (g).

I. The March iCloud Warrant Was Valid.

The March iCloud Warrant permitted the Government to seize the following from the previously obtained iCloud data:

All items that constitutes [sic] evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1512(c) (obstruction of justice) and/or 1519 (destruction of records) involving Timothy MANLY WILLIAMS, Daniel HARRIS, Armando MONTALVO, Patrick BERHAN, Morteza AMIRI, and/or Calvin PRIETO since **October 1, 2019**, including any data that has been deleted but can be recovered or is otherwise available to be restored. These records and materials are more specifically described below:

- (a) Records and communications indicating the obstruction of justice, or attempted obstruction, of any contemplated, reasonably foreseeable, or actual official proceedings;
- (b) Records and communications indicating any contemplated, attempted, or actual destruction, alteration, concealment, and/or falsification of any evidence and/or other records, including text messages, communications, and/or other digital data;
- (c) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crimes under investigation and the account subscriber;
- (d) Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation; and
- (e) Evidence that may identify any co-conspirators or aiders or abettors, including records that help reveal their whereabouts.

(Affidavit in Support of March iCloud Warrant, Attachment B [US-000573].)

1. Probable Cause Supported the March iCloud Warrant.

The Affidavit in Support of the March iCloud Warrant largely repeated the allegations from the February iCloud Warrant, but it sought to expand the scope of the search to include evidence of potential obstruction of justice or destruction of records. As to Amiri, Agent Zoback

added that Amiri “used various messaging applications with end-to-end encryption capabilities,” including Signal and WhatsApp. (Dkt. No. 174-5, Affidavit in Support of March iCloud Warrant, ¶ 54 [US-000561].) In support, Agent Zoback identified several conversations in which Amiri took part or was included.

In April 2020, officers in a group text message conversation which included Amiri switched to Signal out of concern of law enforcement obtaining their messages:

██████████³: Have you guys thought about moving this group chat to one of the disappearing messaging apps like Signal? When SFPD had their multiple text messaging scandals, and several cops got fired, we switched to using those apps. If someone like say, Prieto, gets arrested for rape in Brentwood and BPD dumps his phone, it’ll save us all.

PRIETO: Yea add the app onto here. Make shit easy for us

██████████: The trick is to set a timer for disappearing messages

I don’t think WhatsApp does that

Edward Snowden recommends signal above all others and he would know.

<https://signal.org/install/>

██████████⁴: So are we switching to Signal?

PRIETO: I’m down, that way I can avoid another indictment

██████████: ██████████ ██████████ ██████████ Amiri Calvin ██████████

All added

I created the group already. Let me know when you’re signed up and I’ll add you

██████████: Messages disappear after 30 mins an hour or 6 hours?

What do you recommend?

PRIETO: 6 hours

Some of us be on calls and shit and don’t want to miss the (fire emoji)

³ Officer ██████████ is not a subject of the March iCloud Warrant.

⁴ Officer ██████████ is not a subject of the March iCloud Warrant.

(*Id.* ¶ 65 [US-000566].) The last communication in the group chat was two days later, indicating that Amiri stopped using the group chat out of concern for privacy. (*Id.*) The officers' overt plans to delete their messages after a short period of time further supports an inference that the officers, including Amiri, wanted to evade law enforcement review.

Similar conversations occurred in other group chats in which Amiri was present, including the following March 2021 exchange:

██████████⁵: In light of the wonderful world we all live in, I am going to start a new k9 text thread and leave this conversation and start a new one. I'll add everyone back to it but I suggest we all delete this one. . .

Probably wouldn't be a bad idea going forward to periodically delete and restart just to be safe. Call me out all you want, and I'm just as guilty as the next guy for talking shit but it's overall probably for the best. . .

Ok. Here's the new one. If anyone is like wtf. Please read what I wrote on the old one then delete it.

██████████: I talked with ██████████ pretty extensively about phone downloads, and he said that even shit that's deleted is still saved on the phone. He's even recovered messages sent on Signal in phone dumps. I'm not opposed to starting a new group, but I don't think anyone should have any expectations that old shit will magically disappear. Bottom line, if they get your personal phone, you're already properly fucked. (laughing crying emoji)

██████████: Keep your shit locked and just delete this one is my best bet. I'm blaming ██████████ for it all

██████████: ██████████ said they can get it all through a SW/subpoena from Apple and don't even need the phone if you back up to iCloud. (frowning emoji)

This shit is getting canned. Byyyyyyyyy

(*Id.* ¶ 66 [US-000566-67].)

Agent Zoback provided excerpts from two conversations which he claimed showed Amiri had concerns about law enforcement accessing his messages after Manly's arrest. In May 2021, Rombough warned Amiri that Manly's "phone is tapped." Rombough asked Amiri to come speak

⁵ Officer ██████████ is not a subject of the March iCloud Warrant.

1 to him “outside,” which Zoback interpreted to signal that Rombough did not want to discuss the
2 situation via text in case their phones were tapped. (*Id.* ¶ 67 [US-000567-68].)

3 In one conversation after Manly was placed on administrative leave from the Antioch
4 Police Department, Amiri texted his wife to use Signal to communicate. (*Id.* ¶ 69 [US-000569].)
5 Amiri told his wife that Manly had “messed [Amiri] on signal already” regarding a package
6 inadvertently delivered to Amiri’s home, indicating that Amiri and Manly remained in contact but
7 were wary of law enforcement accessing or reviewing their messages. (*Id.*)

8 These conversations, considered in their totality, support a finding of probable cause that
9 Amiri obstructed justice or destroyed records. Amiri was present in group conversations, backed
10 up to iCloud, in which his fellow officers explicitly discussed the possibility of their records being
11 obtained by law enforcement. In those conversations, officers made plans to ensure that their
12 messages were encrypted and self-erasing. After Manly was placed on administrative leave and
13 the department came under scrutiny, Amiri switched to Signal and WhatsApp to communicate
14 with Manly and encouraged his wife to do the same. The Magistrate Judge thus had a substantial
15 basis to believe there was a “fair probability” that further evidence of Amiri attempting to destroy
16 or hide communications regarding criminal activity could be found in Amiri’s iCloud data.

17 **2. The March iCloud Warrant Was Sufficiently Specific.**

18 As with the February iCloud Warrant, Amiri argues that the March iCloud Warrant was
19 overbroad and insufficiently specific, and that the warrant authorized a general search of his
20 iCloud account. The Court disagrees.

21 **a. The March iCloud Warrant Stated the Scope with Particularity.**

22 The March iCloud Warrant meets the particularity requirement for the same reasons the
23 February iCloud Warrant meets the particularity requirement. Like the February iCloud Warrant,
24 the March iCloud Warrant listed categories of evidence to guide law enforcement’s examination
25 of the data. The categories were cabined by a preambulatory paragraph explaining that the
26 evidence to be seized should indicate obstruction of justice or destruction of records as relating to
27 Amiri and the other named subjects, from October 1, 2019 to the date of the warrant. This was
28 sufficient to limit law enforcement’s discretion.

b. The Scope of the March iCloud Warrant Was Supported by Probable Cause.

As set forth above, Agent Zoback presented the Magistrate Judge with probable cause that evidence of obstruction of justice or destruction of records could be found in the iCloud data. The categories of information provided in the March iCloud Warrant were tailored to evidence of those crimes, state of mind, and identifying the account user and co-conspirators. This scope was narrower than that of the February iCloud Warrant, and it was well-supported by records of conversations in which Amiri and other officers discussed encrypting and deleting messages that reflected potential wrongdoing.

J. The iCloud Warrants Were Lawfully Executed.

Amiri next argues that, even if the warrants were facially valid, they were unlawful in their execution. This argument fails because the challenged evidence was found while officers searched within the scope of the iCloud Warrants.

1. Agent Zoback Did Not Exceed the Scope of the Warrants by Using Observed Messages in Support of Additional Warrants.

Agent Zoback observed evidence of potential crimes outside the scope of seizure permitted by the February iCloud Warrant, and she summarized that evidence in her application for the March iCloud Warrant so that she could lawfully seize the evidence. She repeated this process with the iPhone Warrant and subsequent rollover warrants.

According to Amiri, Agent Zoback necessarily exceeded the scope of the iCloud Warrants when she copied the contents of messages beyond the scope of the warrants' authority to apply for additional warrants. (Dkt. No. 269, Hr'g Tr., 8:4-9, 8:25-9:12.) The Government in turn asserts that nonresponsive data may be used in a request for a rollover warrant without exceeding the bounds of the original warrant.

The Court does not agree that reproducing the content of the challenged text messages in this context constitutes a seizure under the Fourth Amendment. When nonresponsive evidence was apparent, the only way for Agent Zoback to obtain further warrants was to repeat the content of the nonresponsive messages for the Magistrate Judge. There is no evidence suggesting that Agent Zoback otherwise copied the texts. However, even if relaying the substance of the text

1 messages in the warrant applications were a seizure, the seizure would be permissible under the
2 “plain view” doctrine.

3 Both parties agree that *United States v. Wong*, 334 F.3d 831, 836 (9th Cir. 2003), is
4 instructive on this point. In that case, an investigating officer obtained a warrant to search the
5 defendant’s computers, laptops, and mobile devices for evidence of murder (the “January 26
6 warrant”). *Id.* at 834. While executing the January 26 warrant, a computer forensic specialist
7 discovered child pornography. *Id.* at 835. The investigating officer then applied for an additional
8 warrant to search “any and all computer files” for further evidence of child pornography. *Id.*
9 Noting that the question was “a closer call,” the panel found that the January 26 warrant was
10 sufficiently specific. *Id.* at 837-38. The panel then applied the “plain view doctrine” to find that
11 law enforcement lawfully obtained the evidence of child pornography because the officer was (1)
12 “lawfully in the place where the seized item was in plain view; (2) the item’s incriminating nature
13 was ‘immediately apparent;’ and (3) the officer had ‘a lawful right of access to the object itself.’”
14 *Id.* at 838 (quoting *Horton v. California*, 496 U.S. 128, 136-37 (1990)).

15 In this case, Agent Zoback was authorized to review the data for evidence of the alleged
16 steroid scheme. This authorization included reading the text conversations in which the
17 challenged obstruction, degree scheme, and use of force texts were found. The illegal nature of
18 each category of text messages was readily apparent. The objects at issue were the text messages,
19 which were already in the custody of the FBI. All elements of the plain view exception to
20 warrantless searches are satisfied.

21 The Court disagrees with Amiri’s contention that the plain view doctrine has no place in
22 the context of digital data. Certain members of the Ninth Circuit have suggested that the
23 Government should be required to “forswear reliance on the plain view doctrine” when engaging
24 in multi-step digital searches. *CDT*, 621 F.3d at 1178 (Kozinski, J., concurring). In the years
25 since *CDT*, the Ninth Circuit has not adopted this bright line rule. *See, e.g., Schesso*, 730 F.3d at
26 1043 (finding “absence of precautionary search protocols, suggested as guidance in the plurality’s
27 concurring opinion in *CDT III*, was not fatal”). This take on the plain view doctrine appears at
28 odds with the Ninth Circuit’s application of the doctrine in *Wong*. *See Wong*, 334 F.3d at 836

(applying plain view doctrine to evidence of child pornography seized during search of computer for evidence of murder).

2. Agent Zoback Did Not Exceed the Scope of the Warrants by Examining Amiri's Messages with Individual-1.

Amiri contends that the iCloud warrants were unlawful as executed for the additional reason that Agent Zoback examined Amiri's messages with Individual-1, a third-party not named in the iCloud Warrants. (*See* Mot. at 14:14-17 ("But for law enforcement's far flung rummaging through text messages they had no authorization to review, law enforcement would not have obtained any evidence regarding the alleged University Degree Scheme.")) At oral argument, Amiri clarified that it is not his position that the iCloud Warrants limited the scope of the search to communications between the named iCloud account holders. (Hr'g Tr., at 14:10-21.)

The iCloud Warrants authorized Agent Zoback to examine the contents of messages between Amiri and Individual-1. Agent Zoback was authorized to find and seize "communications indicating the possession, use, purchase, sale, distribution, transfer, and/or concealment of controlled substances," which the Magistrate Judge agreed were likely to be found in Amiri's iCloud data. Amiri had previously resided with Individual-1 during the period at issue, and Individual-1 was the romantic partner of another officer suspected to be illicitly trafficking the steroids. It was reasonable to believe that Amiri and Individual-1 would have communicated regarding the steroid scheme. Agent Zoback acted within the scope of the warrant by reviewing messages between Amiri and Individual-1 for communications relating to controlled substances. When she encountered unexpected messages relating to other potential crimes, Agent Zoback properly sought warrants in order to further examine those messages. (*E.g.*, Affidavit in Support of First April 2022 Warrant, ¶¶ 25-38 [US-000887-91].)

K. The iPhone Warrant Was Valid.

The Magistrate Judge issued a warrant to search Amiri's person, mobile phone, iPhone, Apple Watch, and home. (Dkt. No. 174-6, "iPhone Warrant," Attachment A [US-000385-89].) The warrant permitted the Government to seize "evidence, fruits or instrumentalities" of the Target Offenses. (*Id.*, Attachment B [US-000390].) It set forth ten paragraphs describing the

targeted records and materials:

- (1) Records and communications indicating the possession, use, purchase, sale, distribution, transfer, theft, and/or concealment of controlled substances (including steroids), including books, receipts, notes, ledgers, pay and owe sheets, correspondence, records noting price, quantity, date and times when controlled substances were purchased, possessed, transferred, distributed, sold or concealed;
- (2) Records and communications indicating any improper influence on official acts or services, including the receipt, sending, and/or contemplation of any benefits, bribes, and/or kickbacks in exchange for any official acts or services;
- (3) Controlled substances, and evidence of controlled substances (including packaging, baggies, and cutting agents);
- (4) Financial, income, and/or transaction records, whether in electronic or physical record form, and communications about financial transactions;
- (5) Records and communications concerning the potentially excessive use of force by police officers;
- (6) Records and communications indicating the obstruction of justice, or attempted obstruction, of any contemplated, reasonably foreseeable, or actual official proceedings concerning the above categories;
- (7) Records and communications indicating any contemplated, attempted, or actual destruction, alteration, concealment, and/or falsification of any evidence and/or other records concerning the above categories, including text messages, communications, and/or other digital data;
- (8) Records reflecting or relating to co-conspirators, including personal notes, correspondence, cables, personal address lists, listings of telephone numbers, and other items reflecting names, addresses, telephone numbers communications, and illegal activities of associates and co-conspirators;
- (9) Computers or storage media used as a means to commit the violations described above, including the Target Offenses;
- (10) For any computer or storage medium whose seizure is authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant. . . : [evidence regarding the identity of the users, presence or absence of malicious software, the users' state of mind, records of Internet activity, etc.]

(*Id.* [US-000390-92].)

The iPhone Warrant specified that law enforcement personnel could require Amiri to unlock his iPhone and other personal electronic devices with his biometric signature or facial recognition but did not authorize the personnel to obtain Amiri's passcode. (*Id.* [US-000392].) It included the Northern District of California's "Computer Search Protocol," which requires law enforcement to "make reasonable efforts to use methods and procedures that will locate and

1 expose those categories of files, documents, or other electronically-stored information that are
2 identified with particularity in the warrant, while minimizing exposure or examination of
3 irrelevant ... files to the extent reasonably practicable.” (*Id.*, Attachment C ¶ 8 [US-000393].)

4 As with the iCloud Warrants, the parties do not dispute that the iPhone Warrant was issued
5 by a neutral magistrate judge. Therefore, the Court considers whether the warrant was supported
6 by probable cause and whether it described the places to be searched and items to be seized with
7 particularity.

8 **1. Probable Cause Supported the iPhone Warrant.**

9 By the time Agent Zoback applied for the iPhone Warrant, her searches of Amiri’s iCloud
10 for evidence of the steroid scheme and obstruction of justice had unearthed messages relating to
11 the degree scheme and violations of rights under color of law. Agent Zoback’s affidavit provided
12 probable cause for the warrant.

13 **a. The Steroid Scheme.**

14 Agent Zoback reiterated the previous allegations against Amiri regarding the steroid
15 scheme. She added that Amiri’s iCloud messages revealed that Amiri had received five packages,
16 likely containing testosterone, from “[REDACTED].” (*Id.* ¶ 81 [US-000447-48].) [REDACTED]
17 [REDACTED] was located in Florida, and Zoback believed a Florida doctor “would not
18 reasonably be able to offer physicals to customers outside of Florida.” (*Id.* ¶ 82 [US-000448].)
19 Zoback believed any prescription for testosterone for Amiri was therefore likely to be fraudulent.
20 (*Id.*) Zoback further pointed to a text message conversation between Amiri and Berhan in which
21 Amiri provided the information for [REDACTED] and stated “I got free shit for you.” (*Id.*
22 ¶ 84 [US-000479].) Agent Zoback interpreted this text as Amiri offering Berhan free steroids.
23 (*Id.*)

24 Also before the Magistrate Judge was a conversation between Amiri and Manly in which
25 the two officers (apparently jokingly) suggested killing or arresting the Mayor of Antioch
26 (“Lamar”) out of concern that the Mayor would implement drug tests for police officers:

27 AMIRI: Part of Lamar’s drug reform will include drug test

28 MANLY: Broooooooooooooooooooooo Wtf

1 AMIRI: Annual mental health evaluation for each Officer to see if we
are fit for duty This dude is trippin Test for steroids too

2 MANLY: Steroids?

3 AMIRI: Yea as part of the drug test LOL. This dude tryna spend hella
4 extra money out of the existing budget

5 MANLY: We got a kill him HaHaHa

6 AMIRI: Bro! This dude lost his mind

7 MANLY: Seriously bro

8 I'm speechless

9 Well fuck me then lol

10

11 Bro you think they will approve Lamar's proposal on the
steroids? Haha

12 AMIRI: Yea I think they will. Since they can't say no to everything
13 and that pro a little one they will just say yes to I need to get
that dude in 11-5 arrest⁶ asap

14 MANLY: Man I really hate him now

15 AMIRI: Yea bro it's bad

16 (*Id.* ¶ 35 [US-000457-58-].) Based on this conversation, the communications with [REDACTED]
17 [REDACTED], and the reiterated conversations which supported the February iCloud Warrant, the
18 Magistrate Judge had a substantial basis to conclude that evidence of the steroid scheme could be
19 found in Amiri's iPhone.

20 **b. Obstruction of Justice and Destruction of Records.**

21 Agent Zoback reiterated that Amiri had encouraged his wife to switch to Signal after
22 Manly was placed on administrative leave. Further, no messages were found referencing steroids
23 or reflecting Amiri's purchases from [REDACTED] after Manly's arrest—the point at
24 which Amiri switched to communicating with Manly via Signal. (*Id.* ¶¶ 85, 93 [US-000479-80,
25 483].) From this, Agent Zoback believed that Amiri continued to purchase, use, and sell steroids,
26 but did so without using iMessages in order to avoid detection. (*Id.* ¶ 94 [US-000483].)

27 _____
28 ⁶ Agent Zoback stated that an "11-5 arrest" is an arrest for violation of California Highway and
Safety Code section 11550, being under the influence of a controlled substance. (*Id.*)

The Magistrate Judge reasonably could have believed that further evidence of obstruction of justice or destruction of records could be found on Amiri's iPhone.

c. Violation of Rights.

Agent Zoback provided the following exchange between Amiri and Manly, in which Amiri and Manly joked about Rombough using excessive force while Manly watched:

AMIRI: Why do I think of romba when I see this? (crying laughing emoji) (Sends TikTok video from @traproom1 with caption "Officer damages private property while executing a search warrant" of a uniformed police officer ramming a swinging door into the side of a care parked inside of a private garage)

MANLY: Bro a 100% (7 crying laughing emojis) He 40'd another person today

AMIRI: (Smiley face with sunglasses emoji) Deserved?

MANLY: No (crying laughing emoji)

AMIRI: Jesus lol

MANLY: Bro we just shook our heads like WTF... We assisted Patrol on a 602

AMIRI: (Surprised emoji) No way lol Did he at least sit on the dude?

MANLY: It was stupid I know the patrol guys really didn't want any paper work out of it

(*Id.* ¶ 36 [US-000459].) This conversation creates a reasonable expectation that evidence of officers engaging in the improper use of force or violation of rights could be found on Amiri's iPhone, even if the conversation does not necessarily create probable cause that Amiri himself was engaging in such acts. In particular, Amiri and Manly appear to have used their phones to discuss Rombough's alleged pattern of using excessive force, including near-contemporaneous witness accounts. The Magistrate Judge therefore did not clearly err in finding probable cause to search Amiri's iPhone for evidence of excessive force or violation of rights.

2. The iPhone Warrant Was Sufficiently Specific.

a. The March iCloud Warrant Stated the Scope with Particularity.

The iPhone Warrant, like the iCloud Warrants, listed categories of evidence to guide law enforcement's examination of the data. A preamble paragraph explained that the evidence to

be seized was that which indicated the Target Offenses (the steroid scheme, obstruction of justice or destruction of records, and excessive use of force) as it related to Amiri and the other named subjects, from October 1, 2019 to the date of the warrant. (iPhone Warrant, Attachment B [US-000390].) Law enforcement officers had more than enough guidance to limit their discretion in executing the warrant.

b. The Scope of the March iCloud Warrant Was Supported by Probable Cause.

As set forth above, Agent Zoback presented the Magistrate Judge with probable cause in support of each primary bucket of evidence to be seized by the Government. The categories of information provided in the iPhone Warrant permitted the Government to seize evidence of those crimes, evidence relating to Amiri's state of mind, and information identifying the account user and co-conspirators.

L. The Government Did Not Violate *Miranda* When Agent Templin Solicited Defendant's Passcode.

The Government concedes that the iPhone Warrant did not authorize seizure of Amiri's iPhone passcode. Accordingly, the issue before the Court is whether Amiri voluntarily provided his passcode, and whether Agent Templin was required to *Mirandize* Amiri prior to soliciting the passcode. The Court finds that Amiri was not in custody and, even if he were in custody and subject to *Miranda*, the fruits of Amiri's passcode should not be suppressed.

FBI agents interviewed Amiri at the Antioch Police Department. (Amiri Tr., at 1.) Before reading Amiri his rights pursuant to *Miranda v. Arizona*, 384 U.S. 436 (1966), Special Agent Krystal Templin solicited Amiri's iPhone passcode in the following exchange:

TEMPLIN: Before we kind of jump into things, I just want to kind of level with you up front. We do have a search warrant for your phone and any other devices on you today. I'll go over all of that, and then we can kind of talk about --

AMIRI: What?

TEMPLIN: -- what all of this is regarding. So do you have your cell phone on you right now, or is that something we will need to grab?

AMIRI: What's going on?

TEMPLIN: Absolutely. I will certainly fill you in on all of that.

We can kind of start with this. We have a search warrant for the device. So I just want to make sure we kind of cover that piece first. If it is on you, I'm going to have Joyce go ahead and grab it now. . . . We do have biometrics on this particular warrant, so we are going to ask that you unlock the device for us, preferably. If you wouldn't mind handing it over to Joyce, we'll just have --

AMIRI: What is going on? Can I hear some --

TEMPLIN: Absolutely. So --

AMIRI: I'm going to cooperate --

TEMPLIN: No, no. I appreciate that. And I'm sorry to kind of jump in. I wanted to grab the phone first because Joyce is actually going to leave us, and then we'll continue kind of chatting.

Do you mind giving Joyce your pin so that she can --

AMIRI: Yes. It is [PIN].

TEMPLIN: Okay. Perfect. And then we are going to chat over everything else. I'm sorry to . . .

AMIRI: What is going on?

TEMPLIN: So formality only. Before we dive into exactly what is going on, I'm just going to go over Miranda. You do not have to talk to me, but I want to make sure that it is covered up front before we dive into anything.

(*Id.* at 3:1-19, 3:25-5:1.)

1. The Passcode May Be Admitted Because Amiri Was Not in Custody.

Law enforcement officers must provide *Miranda* warnings before interrogation only if the suspect is "in custody." *United States v. Kim*, 292 F.3d 969, 973 (9th Cir. 2002). Whether an individual is in custody is a mixed question of law and fact. *Id.* "[C]ustody" is a term of art that specifies circumstances that are thought generally to present a serious danger of coercion." *Howes v. Fields*, 565 U.S. 499, 508-09 (2012). An individual is in custody if, "in light of 'the objective circumstances of the interrogation,' . . . a 'reasonable person would have felt he or she was not at liberty to terminate the interrogation and leave.'" *Id.* at 509 (quoting *Stansbury v. California*, 511 U.S. 318, 322-23 (1994) and *Thompson v. Keohane*, 516 U.S. 99, 112 (1995)) (internal marks

1 omitted).

2 Among the factors relevant to the custody inquiry are “(1) the language used to summon
3 the individual; (2) the extent to which the defendant is confronted with evidence of guilt; (3) the
4 physical surroundings of the interrogation; (4) the duration of the detention; and (5) the degree of
5 pressure applied to detain the individual.” *Kim*, 292 F.3d at 973 (quoting *United States v. Hayden*,
6 260 F.3d 1062, 1066 (2001)).

7 The first *Kim* factor appears to cut both ways. According to Amiri, his supervisor
8 Lieutenant Fortner ordered Amiri to accompany him after Amiri arrived to start his shift. “When
9 Mr. Amiri asked Lieutenant Fortner what was going on, Lieutenant Fortner intimated that it was
10 not good.” (Dkt. No. 204, Reply, at 7:27-28.) Amiri was at his place of employment, as
11 scheduled, and his supervising officer instructed him to follow to a room with FBI agents. The
12 FBI agents did not summon Amiri, and it does not appear that Amiri was threatened or coerced to
13 appear. However, Amiri likely felt compelled to comply with instructions from his supervisor to
14 enter the room.

15 The second *Kim* factor weighs against a finding of custodial interrogation. There was a
16 distinct lack of confrontation with evidence of guilt. Agent Templin confronted Amiri with
17 certain of his phone messages, but most of her questions centered around Manly, Rombough, and
18 [REDACTED]. At no point did Agent Templin pull out a proverbial smoking gun to elicit
19 a confession or other inculpatory statements from Amiri. Indeed, Agent Templin emphasized that
20 she had “reviewed only a tiny bit” of Amiri’s iCloud data and had “done very little research” into
21 [REDACTED]. (*Id.* at 7:17-18, 89:25.) Instead, she sought Amiri’s assistance to fill in the
22 gaps so she could determine whether prosecution was warranted. (*E.g., id.* at 44:11-21 (explaining
23 purpose of interview was to determine if there was “smoke and fire” or “smoke and that’s it”).)
24 Her tone remained friendly and solicitous throughout the interview. *See United States v.*
25 *Bassignani*, 575 F.3d 879, 884-85 (9th Cir. 2009) (finding factor weighed in favor of non-
26 custodial interrogation where interview was “conducted in an open, friendly tone” without officers
27 “attempt[ing] to challenge the defendant’s statements with other known facts suggesting his
28 guilt”) (internal marks and citations omitted).

The third *Kim* factor likewise weighs against a finding of custody because Amiri was interviewed in his workplace. “[A]n interrogation conducted in familiar surroundings weighs against a finding that the defendant was in custody.” *Id.* at 885. “However, . . . isolating the defendant from the outside world largely neutralizes the familiarity of the location as a factor affirmatively undermining a finding of coercion.” *Id.* (quoting *Kim*, 292 F.3d at 977) (internal marks removed). Amiri was cut off from the world in that the FBI agents removed his cell phone, but there is no indication in the record that he was prevented from contacting others. The agent referred to as “Joyce” left the room, as did Agent Templin and Lieutenant Fortner.⁷ The agents did not conduct their questioning in an interrogation room, but rather in an office. Although he was physically separated and “brought to an enclosed . . . room,” the interrogation in a room at his workplace suggests Amiri was not in custody. *Id.* at 886.

The fourth *Kim* factor weighs in favor of finding the interrogation custodial. The Ninth Circuit explained in *Bassignani* that an interrogation of between 45 and 90 minutes was found to be custodial, and thus the two-and-a-half hour interrogation in the case before it was “at the high end.” *Id.* at 886. Here, the interrogation lasted for nearly two hours. However, the *Bassignani* court found that this fourth factor should be accorded less weight where the interview is not a “marathon session designed to force a confession.” *Id.* (quoting *Davis v. Allsbrooks*, 778 F.2d 168, 171 (4th Cir. 1985)). In this case, Agent Templin did not attempt to force a confession, but rather explored Amiri’s side of the story. Accordingly, this factor is entitled to little weight.

The fifth *Kim* factor strongly weighs in favor of finding the interrogation non-custodial. A reasonable person would have believed he was free to terminate the interview at the outset. *See id.* (“We have consistently held that a defendant is not in custody when officers tell him that he is not under arrest and is free to leave at any time.”). Agent Templin was friendly and familiar in tone at the beginning of their interaction. She introduced herself by her first name, and she invited Amiri to sit down as an option, not a mandatory interview. (Amiri Tr., at 2:11-12, 2:22-24 (“If you want

⁷ That Lieutenant Fortner left the room is apparent from Amiri’s later request to speak to his supervisor, (Amiri Tr., at 95:21-25), and his statement that he believed Fortner was “next door,” (*id.* at 110:9-12).

1 to sit down for a quick second, I will let you know kind of what is going on today.”.) After Amiri
2 provided the passcode, Agent Templin *Mirandized* Amiri as a “formality only.” (*Id.* at 4:22.) She
3 told Amiri before and after the *Miranda* warnings that he was not required to talk to her. (*Id.* at
4 4:24-5:17.)

5 Amiri’s statements and tone also indicated that he understood he was not in custody. After
6 hearing the *Miranda* warnings and being told the nature of the investigation, Amiri stated: “I’ll
7 help you guys however you guys need -- searching my phone, I don’t -- I’ll consent to anything. . .
8 I don’t care. I’m completely cooperative with you guys.” (*Id.* at 9:12-20.) Agent Templin then
9 asked if Amiri would “mind” speaking with her that day, and Amiri agreed. (*Id.* at 9:21-25.)
10 Amiri later stated that he “would love to do all this stuff,” such as speaking to Agent Templin and
11 taking a blood test, to let his supervisors know that he was “not doing anything.” (*Id.* at 63:12-
12 14.)

13 Later in the interview, Agent Templin explicitly told Amiri, “You are not going to be
14 detained in any capacity by us.” (*Id.* at 92:6-7.) It was only after this statement that Amiri
15 appeared uncertain about whether he was permitted to leave. He asked if he could speak to his
16 supervisor. (*Id.* at 95:21.) Agent Templin responded that she would “see if they are available,”
17 and left the room. (*Id.* at 95:22-23.) Amiri then asked Agent Trott: “Am I allowed -- I have no
18 phone or anything. Can I use the restroom or get a drink of water at least? I’m getting -- I’m
19 getting dry mouth.” (*Id.* at 98:22-25.) Agent Trott responded that she would “wait until [Agent
20 Templin] comes back.” (*Id.* at 99:1-2.) Amiri did not leave the room to get water. After Agent
21 Templin’s return, Amiri and Agent Templin discussed whether Amiri is allowed to leave in the
22 following exchange:

23 AMIRI: Am I allowed to go home?

24 TEMPLIN: You are not being detained by us.

25 AMIRI: No, no, not like --

26 TEMPLIN: Oh, yeah.

27 AMIRI: -- after this or do I have to wait for --

28 TEMPLIN: If you are going to go there, I will let them know that you

will be arriving.

(*Id.* at 105:23-106:8.) Amiri again asked if he could get water, prompting the following:

AMIRI: The bathroom is right there. I can walk there with you guys.

TEMPLIN: Look, you are not being detained.

AMIRI: I appreciate it. All right. Thank you.

(*Id.* at 110:1-6.) Agent Trott's statement that Amiri should wait until Agent Templin's return to get water is the only hint in the interview that Amiri was held without freedom to leave, and it came after the conclusion of questioning. However, when Agent Templin returned, she reiterated that Amiri was free to go to the bathroom, get water, speak to his supervisor, or go home.

The cumulation of the *Kim* factors supports a finding that Amiri was not in custody. Amiri was brought to the interview by a supervisor rather than the interrogating officers, was in familiar environs, was not confronted with significant evidence of guilt, was not pressured to confess, and was spoken to with respect throughout. Agent Templin asked Amiri's permission to speak with him, and she told him several times that he was not being detained. Therefore, based on the totality of the circumstances, a reasonable person in Amiri's position would believe that he was free to leave.

2. Even if Amiri Were in Custody, The Fruits of the Passcode Should Not Be Suppressed Because Amiri Voluntarily Provided His Passcode.

In *United States v. Patane*, the Supreme Court explained that the purpose of *Miranda* warnings is to protect defendants "against violations of the Self-Incrimination Clause" of the Fifth Amendment. 542 U.S. 630, 632 (2004). "Physical fruit of a voluntary statement" made without the benefit of *Miranda* are non-testimonial and therefore may be admitted. *Id.* If a statement is not voluntary, the physical fruit must be excluded. See *United States v. Booker*, 561 F. Supp. 3d 924, 932 (S.D. Cal. 2021) (excluding contents of phone where officers conditioned receipt of defendant's medication on defendant entering passcode within the officers' sight).

The record is unambiguous that Amiri voluntarily provided his passcode. Amiri offered the code within minutes of entering the room, interrupting Agent Templin to do so. (Amiri Tr., at

1 4:15-17.) Amiri was aware that the warrant for his phone only extended to biometrics, not his
2 passcode. (*Id.* at 3:25.) Amiri reiterated his consent to searching or copying his phone several
3 additional times. He offered to sign a “consent letter,” (*id.* at 48:2-3), to permit the FBI to use a
4 Cellebrite Kit from the Antioch Police Department to speed up the process, (*id.* at 48:22-25), and
5 to “sign a consent” so that the FBI could “download it today,” (*id.* at 92:16-21). Evidence
6 obtained from subsequent searches of the phone is admissible under *Patane*.

7 Amiri argues that, even if the statement was voluntary, the Court should not read *Patane* to
8 extend to the contents of cell phones due to the unique privacy interests implicated by modern
9 smart phones. In support, Amiri cites *Riley v. California*, 573 U.S. 373 (2014).

10 *Riley* involved a warrantless search of a cell phone seized incident to an arrest for
11 possession of concealed and loaded firearms. *Id.* at 378. After the arrest, a detective searched the
12 phone for evidence of possession of the guns. *Id.* at 279. During that search, the detective found
13 photographs of Riley with a car that had been involved in an earlier shooting. *Id.* Riley was
14 subsequently charged with firing at an occupied vehicle, assault with a semiautomatic firearm, and
15 attempted murder. *Id.* The Supreme Court noted that “modern cell phones. . . are now such a
16 pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they
17 were an important feature of human anatomy.” *Id.* at 385.

18 Given the novelty of the technology, and the apparent inapplicability of earlier caselaw
19 regarding searches incident to arrests, the *Riley* Court examined “on the one hand, the degree to
20 which [a warrantless search] intrudes upon an individual’s privacy and, on the other, the degree to
21 which it is needed for the promotion of legitimate governmental interests.” *Id.* The court
22 distinguished between “physical objects” and “digital data,” and it found that a warrantless search
23 incident to arrest was appropriate for the “physical aspects” of a phone but not the data contained
24 within the phone. *Id.* at 386-87.

25 The Court is mindful of *Riley*’s wider implications regarding the massive trove of digital
26 data found within smartphones. Ultimately, however, the Court finds *Riley*’s rationale
27 inapplicable where, as here, a suspect voluntarily and knowingly provides his smartphone
28

passcode to law enforcement officers in order to facilitate their speedier search of the phone.⁸ Amiri's phone was not removed from his pocket during an arrest; he handed it over and provided the passcode after being advised that the FBI had a warrant to search the phone and to use his biometrics to unlock it. To the extent the passcode provided greater access than biometrics alone, *see United States v. Maffei*, 2019 WL 1864712, No. 18-cr-00174-YGR-1, at **13-14 (Apr. 25, 2019) (noting passcode required to change or remove encryption on device), Amiri freely and vociferously consented to that greater access in an attempt to speed the return of his phone. It defies common sense, in this context, to find that the Government is required to refuse to look at the contents of the freely given data.

3. Suppression Is Not Available Because the Disputed Text Messages Were Obtained Through the iCloud Warrants.

Amiri argues that all messages regarding the college degree scheme and excessive use of force were obtained as a result of the supposed *Miranda* violation. Not so. As the Court determined above, the search warrants authorized Agent Zoback to read text messages between the subjects and between Amiri and Individual-1. Therefore, the Government had access to the messages through alternate means.

4. An Evidentiary Hearing Regarding the Passcode Solicitation Is Not Warranted.

Amiri seeks an evidentiary hearing regarding the circumstances in which he provided his iPhone passcode to Agent Templin. Although Amiri vigorously contests that he volunteered his passcode, the Court finds that the transcript and recording unambiguously demonstrate that Amiri's statement was voluntary and that the fruits of the statement should not be suppressed. Moreover, even if the statement was involuntary as Amiri contends, suppression is not an available remedy because the fruits of the password were previously obtained by the FBI through Amiri's iCloud data.

⁸ *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), cited by Amiri, is distinguishable on this basis as well. *Djibo* involved a search incident to an arrest when the defendant was detained entering the United States. *Id.* at 298. The testifying officer could not recall if he asked for the passcode before or after the defendant was arrested and had invoked his right to remain silent. *Id.* at 300-01.

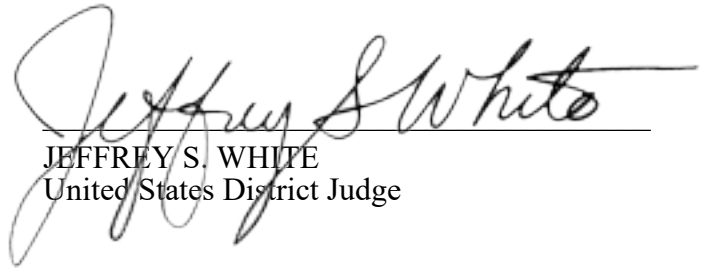
CONCLUSION

For the foregoing reasons, Defendant Amiri's Motions to Suppress are DENIED.

The parties shall file a joint statement regarding whether the Order should remain under seal, including any proposed redactions, within 14 days of this order.

IT IS SO ORDERED.

Dated: July 26, 2024



JEFFREY S. WHITE
United States District Judge